Požadované technické parametry dodávky síťového zařízení

Předmětem dodávky je aktivní síťový prvek dle technických podmínek uvedených níže.

Tabulka povinných požadavků pro aktivní síťový prvek (požadován 1 ks)

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti**
Základní vlastnosti	
Třída zařízení	směrovač, firewall
Formát zařízení	fixní konfigurace, desktop provedení
Montážní přípravek do racku s vyvedením portů dopředu a přichycením napájecího zdroje	ano
Počet 100/1000Base-T portů	10
Sériová konzolová linka	ano
Lokální disk pro ukládání logů	ano
Podporované funkce	
Provoz zařízení v režimu L3 (směrování)	ano
Podpora virtuálních instancí firewallu – plná funkcionalita jednotlivých virtuálních firewallů	ano
Podpora management protokolů SNMP, Syslog, NTP ve virtuální instanci firewallu	ano
Podpora překladu adres NAT/PAT	ano
Podpora protokolu IPv6 pro management, IPv6 tunnelling, firewalling, NAT46, NAT64, IPv6 IPSec VPN	ano
Podpora tunelování GRE a VXLAN	ano
Počet podporovaných VLAN	250
Podpora IEEE 802.1Q	ano
Podpora QoS pro IPv4 a IPv6	ano
Podpora prioritizace provozu na aplikační úrovni (7. vrstva)	ano
Podpora Link Aggregation IEEE 802.3ad/LACP	ano
Vytváření bezpečnostních zón (Zone-based firewall)	ano
DoS/DDoS ochrana	
Dekódovaní DNS, HTTP	ano
Identifikace útočících stanic – prahové hodnoty pro dotazy za časovou jednotku	ano
Akce blokace požadavků, akce snížení počtu požadavků za časovou jednotku	ano
Antispoofingová kontroly Reverse Path Forwarding Check pro IPv4 i IPv6	ano
Ochrana centrálního procesoru (Control Plane) pomocí rate limiterů	ano
Správa a monitoring	
Grafické rozhraní pro kompletní správu firewallu	ano
Textově orientované konfigurační rozhraní (CLI)	ano
Konfigurace zařízení v člověku čitelné textové formě	ano
Povýšení operačního software zařízení po síti pomocí protokolů TFTP, FTP a/nebo HTTP, HTTPS, SFTP/SCP	ano
Možnost nahrání/zálohování textové konfigurace zařízení po síti pomocí protokolů TFTP, FTP a/nebo HTTP, HTTPS, SFTP/SCP	ano
Přístup pomocí protokolu SSHv2	ano

Podpora protokolů SNMPv2, SNMPv3	ano
DNS klient	ano
Podpora synchronizace času protokolem NTPv3	ano
Podpora NetFlow v9, IPFIX nebo ekvivalentních protokolů exportů toků/flow	ano
Ověřování přístupu k zařízení pomocí RADIUS anebo TACACS+ protokolu	ano
Vzdálené logování na syslog server	ano
Systémový rollback konfigurace	ano
Správa revizí konfigurací	ano
Směrovací protokoly	
Směrování pro IPv4 a IPv6 s akcelerací v hardware	ano
Dynamické směrování pro IPv4 (OSPF, BGP)	ano
Dynamické směrování pro IPv6 (OSPFv3, MP-BGP)	ano
OSPF s MD5 a NSSA	ano
Policy-based routing	ano
Statické směrování pro IPv4 a IPv6	ano
Směrování multicastu	
PIM (dense i sparse mód)	ano
PIM pro IPv6	ano
IGMPv2	ano
IGMPv3	ano
IGMPv3 snooping	ano
Bezpečnost	
Statefull firewall	ano
Transparentní (L2) stavový firewall	ano
Možnost rozšíření o rozpoznávání aplikací	ano
Možnost rozšíření o kategorizaci a kontrolu web obsahu	ano
ACL na rozhraní IN/OUT včetně virtuálních – VLAN, loopback, 802.3ad	ano
ACL pro IP	ano
ACL pro ethernetové rámce	ano
ACL podle regulárních výrazů ze záhlaví paketu i vlastních dat	ano
Management	
Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	ano
Možnost omezení přístupu k CLI definováním uživatelských rolí	ano
Podpora managementu stávajícího firewallu	ano
DNS klient	ano
NTP klient s MD5 autentizací	ano
Nástroje pro měření odezev v síti (například IP SLA nebo ekvivalentní)	ano
Výkonnostní parametry	
Minimální agregovaná propustnost firewallu při plném zatížení	6 Gb/s
Maximální zpoždění při plném zatížení	5 µs
Minimální počet současných TCP spojení	500 tisíc
Minimální počet nových spojení	30 tisíc/s
Minimální propustnost IPSec VPN (AES256 + SHA256)	6 Gb/s
Minimální počet IPSec tunelů	200
Počet virtuálních instancí firewallu	10

Další technické požadavky

- Všechny poptávané aktivní síťové prvky musí být z důvodů ochrany stávajících investic a minimalizace celkových nákladů na vlastnictví a provoz počítačové sítě zadavatele kompatibilní se všemi již používanými zařízeními, komunikačními protokoly a systémy správy sítě specifikovanými níže.

Popis stávajícího prostředí počítačové sítě ZČU

Používané komunikační protokoly a podpůrné vlastnosti aktivních prvků sítě ZČU

V akademické síti ZČU WEBnet jsou v současné době používány následující komunikační protokoly a další podpůrné vlastnosti aktivních prvků, s nimiž musí být poptávaná zařízení kompatibilní:

- Podpora IEEE 802.1Q/p (minimálně 1000 VLAN, konfigurační možnosti statického omezování síření VLAN), IEEE 802.1s/w (RSTP/MSTP), IEEE 802.3ad, IGMPv2/v3, MLDv1/v2 a vlastnické L2 protokoly VTPv3, PVRSTP+, CDPv2, UDLD.
- Možnosti ochrany spanning tree protokolu vůči zneužití (filtrace BPDU rámců na jednotlivých rozhraních, kontrola přípustnosti BPDU apod.).
- Podpora agregace linek (LACP nebo PAgP).
- Podpora privátních VLAN (logická izolace jednotlivých rozhraní nebo skupin rozhraní v rámci téže VLAN).
- Podpora omezení (procentuálního poměru) broadcastového a multicastového provozu na rozhraní.
- Duální podpora IPv4 a IPv6 unicast i multicast (možnost současné konfigurace IPv4 a IPv6 adres na tomtéž fyzickém nebo logickém rozhraní, dual-stack).
- Podpora směrovacích protokolů BGPv4, OSPFv2, OSPFv3, PIM-SMv2, RIP, statického směrování a možnosti redistribuce směrovacích informací mezi jednotlivými protokoly, rozkládání zatížení na L3 paralelních cestách, možnosti vytváření logicky oddělených instancí virtuálních směrovacích tabulek v rámci téhož L3 přepínače (podpora virtuálních směrovacích instancí).
- Podpora HSRP nebo VRRP pro zajištění redundance výchozí brány koncovým stanicím/serverům.
- Podpora GRE tunelů.
- Podpora IGMPv2, IGMPv3 a hardwarová podpora omezování zbytečného šíření multicastových rámců/paketů na rozhraní bez explicitních příjemců (IGMPv2/v3 a MLDv1/v2 snooping).

- Možnost definovat povolené MAC adresy na portu, jejich maximální počet na portu a definování různého chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy).
- Hardwarová podpora bezstavové bezpečnostní filtrace provozu podle L2/L3/L4 atributů na úrovni linkové/síťové/transportní vrstvy aplikovatelná na úrovni L2/L3 fyzického i logického rozhraní (VLAN).
- Vzdálený management aktivních prvků (typicky pomocí protokolů Telnet, SSH, HTTP/HTPS nebo SNMPv2/v3).
- Implementace čítačů přenesených bytů/paketů pro jednotlivé relevantní entity síťových informací (typicky rozhraní, filtry apod.) přístupné přes příkazovou řádku a SNMP.
- Možnost nastavení omezení distribuce IP multicastu ve VLAN.
- Možnost ochrany proti útokům na úrovni síťové a linkové vrstvy (IP DHCP Snooping, Dynamic ARP Inspection, IP Source Guard).
- Hardwarová podpora zajištění kvality služby (QoS) podle L2/L3/L4 atributů umožňující implementaci QoS podle modelu rozlišovaných služeb (DiffServ).

Nástroje používané pro správu sítě ZČU

Pro správu sítě ZČU jsou používány následující nástroje síťového managementu, s nimiž musí být poptávaná zařízení kompatibilní.

Správa konfigurací

Zálohování konfigurací všech aktivních komunikačních prvků Cisco je prováděno centrálně automaticky pomocí systému RANCID[1] s webovou nadstavbou Subversion (pro přehledné zobrazování změn) periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je udržována minimálně po dobu jednoho roku. Navíc jsou paralelně zálohovány konfigurace (a jejich přehledných sumárních změny) všech aktivních komunikačních prvků Cisco pomocí systému NeDi[2] periodicky alespoň jednou denně. Archivace (změn) historie konfigurací je opět v systému NeDi udržována minimálně po dobu jednoho roku.
Pro hromadné konfigurace skupin zařízení se využívají systémy Netmanager[3], umožňující paralelní vykonávání příkazů, a NeDi.

Připojení vzdálených lokalit pomocí VPN

Pro připojení vzdálených lokalit ZČU je využíván VPN koncentrátor[4], pro jehož management je používán specializovaný software[5]. Pro sledování a reportování provozních anomálií je používán specializovaný analyzátor[6].

Inventarizace síťových zařízení

Pro inventarizaci veškerých síťových zařízení (typicky aktivních komunikačních prvků a koncových zařízení jako jsou uživatelská PC, notebooky, servery a síťové tiskárny) se využívají dva druhy nástrojů:

- registrační systém Sauron[7] v prostředí sítě ZČU (uživatelé a administrátoři registrují síťová zařízení pomocí služby „hostmaster“) a registrační systém Knet[8] v prostředí kolejní sítě (včetně

[1] http://www.shrubbery.net/rancid/
[2] http://nedi.ch/
[3] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.
[4] Dva NGFW Fortinet Fortigate 3700D zapojené v clusteru.
[5] Virtuální appliance Fortinet FortiManager.
[6] Fortinet FortiAnalyzer 3000E.
[7] http://sauron.jyu.fi/
[8] Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.

funkce řízení přístupu oprávněných uživatelů do sítě na základě konfigurace kolejních DHCP/DNS serverů a pravidel na centrálním kolejním firewallu)

- on-line systémy Netdisco[9] a NeDi, které na základě periodicky získávaných informací z aktivních komunikačních prvků pomocí protokolů SNMP a CDP poskytují informace o zařízeních připojených do sítě (např. počty, typy a verze OS aktivních prvků, informace o topologii sítě, VLAN, IP podsítích, bezdrátových SSID, mapování MAC adres na IP adresy, připojení MAC/IP adres za konkrétními fyzickými porty jednotlivých přepínačů, informace o SMB atd.[10]) s možností pokročilého vyhledávání (např. nalezení fyzického připojení zařízení s danou IP/MAC adresou, nalezení duplicitních MAC/IP adres apod.), včetně uchovávání stavové historie.

Monitorování provozu

Provozní trendy

Pro sledování non-stop dostupnosti na úrovni služeb se používá systém Icinga[11], který je současně také využíván pro monitorování dostupnosti všech aktivních komunikačních prvků a služebních/management serverů, včetně konfigurace automatického upozorňování/eskalace e-mailem při detekci problémové/chybové situace.

Pro non-stop historii sledování základních L2 provozních charakteristik aktivních komunikačních prvků všech prostředí pomocí SNMP[12] (typicky zatížení CPU, obsazení operační paměti, stav napájecích zdrojů, teplota, počet BGP prefixů a stavové informace jednotlivých portů/rozhraní jako počet přenesených bytů/rámců/paketů, chybovost portů/rozhraní atd.) se používá optimální konfigurace dvojice nástrojů Cricket[13] a Torrus[14] pracujících nad RRD databázemi.

Pro sledování provozu na úrovni L3/L4 datových toků se využívá technologie NetFlow v9. NetFlow informace exportované ze směrovačů a linuxových firewallů (kolejní extranet) se zpracovávají pomocí produkčního IPv4/IPv6 software FTAS[15].

Pro monitorování historie latence/jitteru/ztrátovosti paketů (typicky VoIP subsystému) se používá aktivní nástroj Smokeping[16].

Pro monitorování problémových provozních stavů se používá standardní mechanismus zpracování nevyžádaných deníkových zpráv generovaných aktivními prvky na bázi protokolu Syslog a SNMP trap, přičemž se navíc využívá i nadstavba Zenoss Core[17] pro inteligentní korelaci trapů.

Bezpečnostní monitorování

Pro monitorování síťové bezpečnosti se jednak využívají standardní nástroje Syslog a SNMP trapy, které mohou být ještě dále inteligentně předzpracovány/filtrovány, korelovány a reportovány SIEM systémem zpracování Syslog hlášení z aktivních prvků OSSEC[18] a pro SNMP trapy systémem Zenoss Core.

Vynucování bezpečnostní síťové přístupové politiky umožňující centralizované systémové zablokování přístupu problémových uživatelů do sítě či síťových služeb (blacklist) zejména na úrovni L2 VACL nebo L3 ACL případně ještě s kombinací vypnutí daného portu na přístupovém prvku (typicky nejblíže

---

[9] http://www.netdisco.org/

[10] Z bezpečnostních důvodů se však záměrně nevyužívají integrované služby manipulace se stavy portů přepínačů vyžadující SNMP přístup pro zápis.

[11] http://www.icinga.org/

[12] Konfigurace aktivních prvků pouze v režimu pro čtení s povolenými IP adresami management stanic dle ACL.

[13] http://cricket.sourceforge.net/

[14] http://torrus.org/

[15] http://www.cesnet.cz/doc/techzpravy/2004/ftas-arch/,
http://www.cesnet.cz/doc/techzpravy/2006/ftas-interface/,
http://www.cesnet.cz/akce/2009/zazemi-pro-cert-csirt/p/sledovani-provozu.pdf

[16] http://oss.oetiker.ch/smokeping/

[17] http://www.zenoss.com/solution/network-monitoring

[18] http://www.ossec.net/

místu svého vzniku podle typu komunikačního prvku) je řízeno pomocí nástroje NetSpy[19]. Tento vlastní nástroj také poskytuje další potřebné podpůrné administrátorské funkce jako např. automatickou detekci neregistrovaných zařízení, vyhledání různých konfliktních síťových stavů, management VLAN/IP podsítí atd.
Vzdálený administrátorský přístup ke všem aktivním síťovým prvkům je zajištěn pouze pomocí SSH protokolu s autentizací/autorizací protokolem TACACS+ z předdefinovaných povolených bezpečných podsítí/IP adres. Management rozhraní L2 přepínačů je umístěno ve vyhrazené IP podsíti chráněné firewallem. Pro L3 přepínače/směrovače je konfigurována ochrana Control Plane Policing/CoPP, pokud tuto vlastnost podporují. AAA auditní informace o administrátorských přístupech ke konfigurovaným zařízením je k dispozici na TACACS+ serverech CIV ZČU.

[19]Vlastní otevřený systém založený na využití výsledků diplomových prací studentů FAV.